Modèle de Défaillance lié à la Sûreté pour des Applications Ferroviaires Critiques - Développement à Base de Composants

Marc Sango, Laurence Duchien, Christophe Gransart

Modèle de Défaillance lié à la Sûreté pour des Applications Ferroviaires Critiques

Développement à Base de Composants

Marc Sango, Laurence Duchien, Christophe Gransart
Univ Lille Nord de France - IFSTTAR - INRIA - Univ Lille 1 - LIFL, UMR CNRS 8022
marc.sango@ifsttar.fr, laurence.duchien@inria.fr, christophe.gransart@ifsttar.fr

Contexte

Les applications critiques sont conçues de telle façon qu'elles continuent à fonctionner en conformité avec leurs spécifications de sûreté malgré des fautes résiduelles. Cette technique de conception est connue sous le nom de la tolérance aux fautes. La tolérance aux fautes comprend plusieurs modes de défaillances qui sont définis par leurs sémantiques d'interprétation.

Dans certains domaines critiques comme dans le ferroviaire, **les applications restent en grande majorité développées manuellement et les différentes préoccupations extra fonctionnelles, telle que la tolérance aux fautes, sont intégrées dans le code fonctionnel** sous forme d'algorithmes, de protocoles, et ou encore d'exceptions.

Construites ainsi, les architectures logicielles de ces applications sont complexes à faire évoluer et encore plus difficiles à adapter à l'exécution.

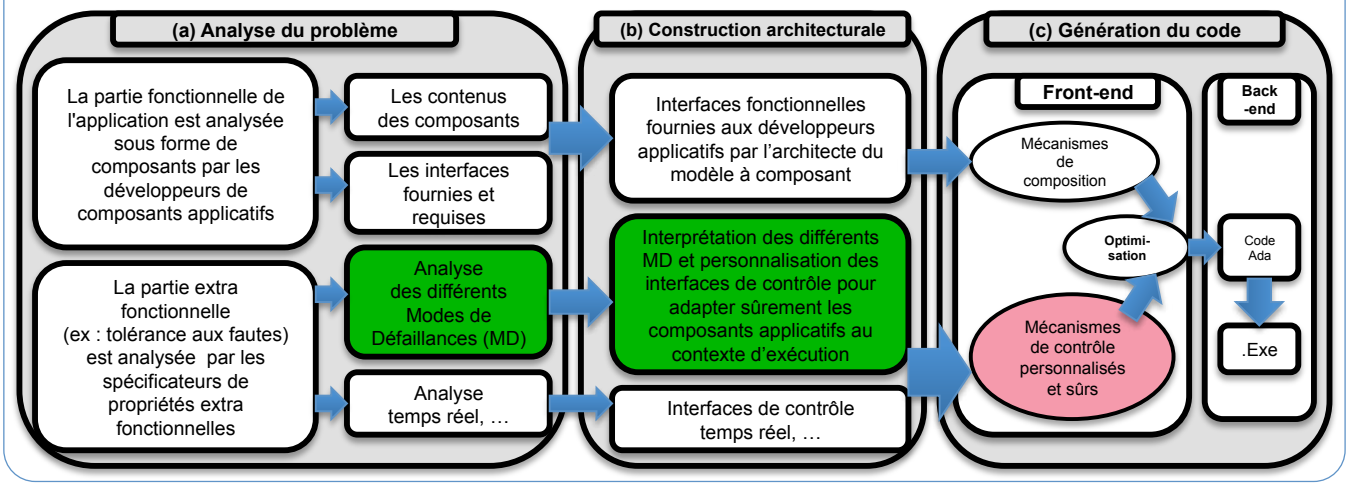
Objectif, approche et proposition

Objectif : Séparation de préoccupations dans tout le cycle de vie logiciel pour préserver les propriétés de sûreté de la conception à l'exécution.

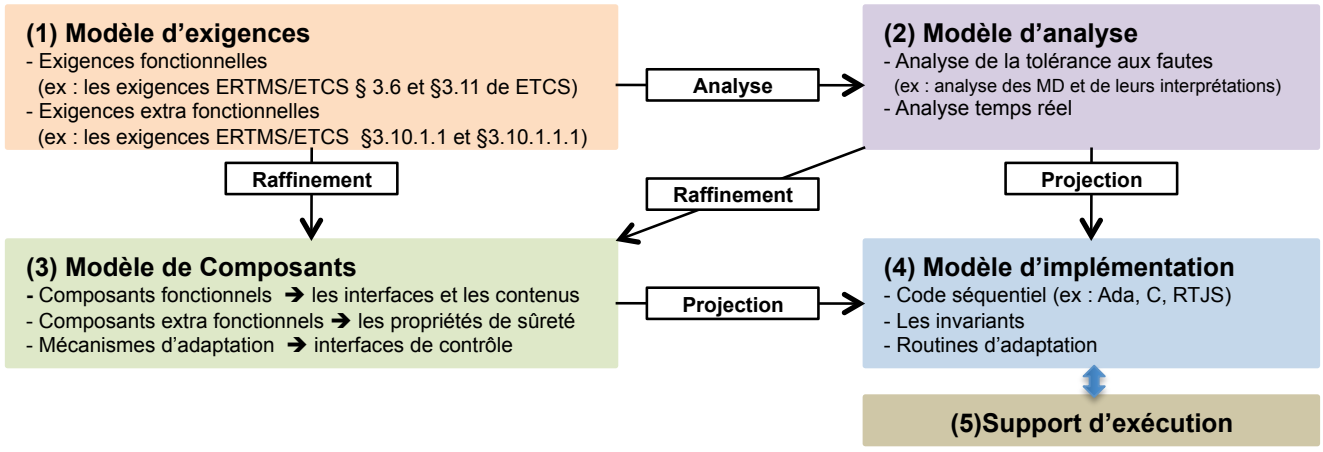
Approche : Séparation des préoccupations des fonctionnalités classiques des fonctionnalités de tolérances aux fautes, i.e., définition des différents modes de défaillance qui impactent la sûreté de fonctionnement et interprétation de la conséquence de ces défaillances.

Proposition : Utilisation d'une approche à base de composants qui mettra en œuvre la séparation des préoccupations de la conception à l'exécution.

Approche générale



Méthodologie de développement



Plan de travail

- Définition d'un modèle de composants comportant le modèle de défaillances amélioré et qui permettra de réaliser la séparation de préoccupations jusqu'à l'exécution
- Implémentation du modèle dans un langage recommandé dans le domaine ferroviaire
- Expérimentation sur un exemple ERTMS/ETCS

Conclusion

- Proposition d'un modèle de modes de défaillances et de leurs interprétations
- Évaluation du système ERTMS/ETCS et Norme Ferroviaire EN 50128
- Évaluation de Fractal

Références

- A. Bondavalli and L. Simoncini. Failure classification with respect to detection. In Distributed Computing Systems, 1990. Proceedings., Second IEEE Workshop on Future Trends of, pages 47 –53, sep-2 oct 1990.
- M. Stoicescu, J.-C. Fabre, and M. Roy. From design for adaptation to component-based resilient computing. In PRDC, pages 1–10, 2012.